UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/518,301	12/17/2004	Julien Stern	0505-1038	6997

466 7590 08/22/2008

YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/518,301	**Applicant(s)** STERN ET AL.	
	Examiner CARL COLIN	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _17 December 2004_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-23_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-23_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _17 December 2004_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _see attached_.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. Pursuant to USC 131, claims 1-23 are presented for examination.

Priority

2. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 12/17/2004 is being considered by the examiner.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2, 12, and 13 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 2 recites said encrypted cryptographic data ($F_{KP}(D_A)$). There is insufficient antecedent basis for this limitation in the claim.

Claims 12-13 recite the limitation "said content data". It is not clear which content data applicant is referring to. There is insufficient antecedent basis for this limitation in the claims.

Claim Objections

5. Claim 10 is objected to because of the following informalities: "the image" should be replaced by --an image--. Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-6, 11-13, 16-18, and 20-23 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,424,718 to **Holloway**.

As per claim 1, **Holloway** discloses a method for the on-line exchange of content data in a secure manner, comprising the steps consisting in: **Holloway** discloses a client device connected to a system server 130 comprises at least two servers (see fig.1) through a network and discloses receiving a pass phrase (code) entered by a user the user at the client device (see column 8, lines 15-23 and column 9, lines 10-18) that meets the recitation of *receiving (32) a code entered by a user in an interface device (4a-c, 50) linked to a first server device (3) by at* *least one data network (1, 54),* **Holloway** discloses sending a message for transaction services (see column 9, lines 10-18) to a system server in which is stored users cryptographic data encrypted with users' pass phrase (see column 7, lines 30-53) that meets the recitation of *sending (36) a read request from said interface device to said first server device in which is stored the respective personal cryptographic data of a plurality of users, said personal cryptographic data of each user being encrypted using a respective authentic code of said user,* **Holloway** discloses *receiving (42) the encrypted personal cryptographic data of said user in said interface device,* (see column 9, lines 18-26); **Holloway** discloses requesting user to enter the pass phrase to allow deciphering of the cryptographic data (see column 9, lines 18-26) that meets the recitation of *decrypting (44) said personal cryptographic data using said entered code when said entered code corresponds to said authentic code of the user, characterized in that it comprises the steps consisting in:* **Holloway** further discloses using the private key to exchange messages with server system or a separate system to server 130 that meets the recitation of *using (46) said personal cryptographic data to protect an exchange of content data (58, 60, 66, 68, 76) between said interface device and at least one second server device (2a-c) linked to said interface device by at least one data network,* **Holloway** also discloses that the pass phrase may also used as a key and stored in client as key or hashed (see column 8, lines 18-23, and lines 45-50) and erasing the algorithms and keys from the client (see column 7, lines 57-61 and column 10, lines 64-65) that meets the recitation of *erasing (48) said entered code and said personal cryptographic data from said interface device.*

As per claim 2, **Holloway** discloses sending cryptographic data to the client through a secure communication channel between the client and the server and sharing at least one encryption key (Ks) that meets the recitation of characterized in that said interface device and said first server device set up a confidential communication channel between themselves by sharing at least one encryption key (Ks) offering a high degree of entropy in relation to said authentic code of the user, said encrypted personal cryptographic data (F.sub.KP(D.sub.A)) being transmitted to said interface device via said confidential communication channel (see column 7, lines 30-47 and column 9, lines 47-55).

As per claim 3, **Holloway** discloses generating a hash message of the authentication code of the user using a one-way hash function stored at the server device for verification and authentication of the client (see column 8, line 26 through column 9, line 10) that meets the recitation of characterized in that at least one item of personal code verification data (VP) deriving from said authentic code of the user (P) according to a deterministic function (h(N//.)) is stored in said first server device and in that said first server device explicitly or implicitly authenticates the interface device using said personal code verification data item.

As per claim 4, **Holloway** discloses characterized in that said deterministic function is a collision-resistant, irreversible function (see column 8, lines 26-66).

As per claim 5, **Holloway** discloses characterized in that said interface device and said first server device simultaneously handle the sharing of said at least one encryption key and the explicit or implicit authentication of said interface device by said first server device using a Password-Based-Key-Exchange (PBKE) protocol (see column 7, lines 30-47; column 9, lines 47-55 and column 8, lines 1-11).

As per claim 6, **Holloway** discloses characterized in that said Password-Based-Key-Exchange type protocol includes a single communication in each direction between said interface device and said first server device, said communication from the first server device to the interface device including the transmission of the encrypted personal cryptographic data (see and column 8, lines 1-11 and column 8, line 26 through column 9, line 10).

As per claim 11, **Holloway** discloses the server system may comprise of multiple server computers (see column 6, lines 41-48) that meets the recitation of second server and further discloses a separate system to server system (see column 9, lines 55-60) that also meets the recitation of second server **Holloway** discloses the client performs secure communication with the second server using key in the cryptographic data to perform digital signature for authentication (see column 9, lines 45-65).

As per claim 12, **Holloway** discloses receiving content data entered by said user in said interface device, encrypting said content data using at least one encryption key included in said personal cryptographic data, sending said encrypted content data (58, 66) to said at least one second server device (2a-b) to store said encrypted content data in said second server device and/or transmit it to a recipient (see column 9, line 45 through column 10, line 26).

As per claim 13, **Holloway** discloses sending a second read request specifying content data from said interface device to said at least one second server device (2a), receiving said encrypted content data (60) from said at least one second server device in said interface device, decrypting said content data using at least one decryption key included in said personal cryptographic data (see column 9, line 45 through column 10, line 26 the message includes decryption key for decrypting content data).

As per claim 16, **Holloway** discloses characterized in that it comprises the step consisting in: checking the integrity of the personal cryptographic data received from said first server device using integrity control data attached to said personal cryptographic data received from said first server device (see column 9, lines 26-38).

As per claim 17, **Holloway** discloses a registration interface device (4a-c, 50), characterized in that it comprises: **Holloway** discloses *providing (11, 12) personal cryptographic data in said interface device* (see column 9, lines 18-26); **Holloway** discloses a client device connected to a system server 130 comprises at least two servers (see fig.1) through a network and discloses receiving a pass phrase (code) entered by a user the user at the client device (see column 8, lines 15-23 and column 9, lines 10-18) that meets the recitation of *receiving (14) an authentic code entered by said user in said interface device*, **Holloway** discloses *encrypting (20) said personal cryptographic data using said authentic code* (see column 9, lines 18-26);sending from a system server in which is stored users cryptographic data encrypted with users' pass phrase (see column 7, lines 30-53) that meets the recitation of *sending (24) said encrypted personal cryptographic data from said interface device to a first server device (3) to store said encrypted personal cryptographic data in said first server device;* **Holloway** also discloses that the pass phrase may also used as a key and stored in client as key or hashed (see column 8, lines 18-23, and lines 45-50) and erasing the algorithms and keys from the client (see column 7, lines 57-61 and column 10, lines 64-65) that meets the recitation of *erasing (28) said personal cryptographic data and said authentic code from said interface device.*

As per claim 18, **Holloway** discloses characterized in that the registration step comprises the steps consisting in: forming (18) personal code verification data from said authentic code, sending (24) said personal code verification data from said interface device to said first server device to store said personal code verification data in said first server device (see column 8, lines 15-35).

As per claim 20, **Holloway** discloses interface device (4a-c, 50) for the on-line exchange of content data in a secure manner, comprising: **Holloway** discloses a client device connected to a system server 130 comprises at least two servers (see fig.1) through a network and discloses receiving a pass phrase (code) entered by a user the user at the client device (see column 8, lines 15-23 and column 9, lines 10-18) that meets the recitation of *a means for receiving (32) a code entered by a user;* **Holloway** discloses sending a message for transaction services (see column 9, lines 10-18) to a system server in which is stored users cryptographic data encrypted with users' pass phrase (see column 7, lines 30-53) that meets the recitation of *a means for sending (36) a* *first read request from said interface device to a first server device (3) in which respective personal cryptographic data of a plurality of users is stored, said personal cryptographic data of each user being encrypted using a respective authentic code of said user,* **Holloway** discloses *a means for receiving (42) the encrypted personal cryptographic data of said user* (see column 9, lines 18-26); **Holloway** discloses requesting user to enter the pass phrase to allow deciphering of the cryptographic data (see column 9, lines 18-26) that meets the recitation of *a means for decrypting (44) said personal cryptographic data using said entered code when said entered code corresponds to said authentic code of the user, characterized by:* **Holloway** further discloses using the private key to exchange messages with server system or a separate system to server 130 that meets the recitation of *means for using (46) said personal cryptographic data to protect an exchange of content data (58, 60, 66, 68, 76) between said interface device and at least one second server device (2a-c),* **Holloway** also discloses that the pass phrase may also used as a key and stored in client as key or hashed (see column 8, lines 18-23, and lines 45-50) and erasing the algorithms and keys from the client (see column 7, lines 57-61 and column 10, lines 64-65) that meets the recitation of *a means for erasing (48) said code and said personal cryptographic data from said interface device.*

As per claim 21, **Holloway** discloses the client comprises a cryptographic module (see column 6, lines 13-41) with means for signing, encrypting and/or decrypting that meets the recitation of characterized in that it consists of an electronic mail management program, said means of using the personal cryptographic data comprising a cryptographic module for signing, encrypting and/or decrypting electronic mail using at least some of said personal cryptographic data (see column 8, lines 63-65 and column 9, lines 23-26, 45-55).

As per claim 22, **Holloway** discloses the client comprises a cryptographic module (see column 6, lines 13-41) with means for signing, encrypting and/or decrypting that meets the recitation of characterized in that it consists of a plug-in module suited to an electronic mail management program comprising a cryptographic module for signing, encrypting and decrypting electronic mail, said means of using the personal cryptographic data comprising a means for providing said cryptographic module with at least some of said personal cryptographic data (see column 8, lines 63-65 and column 9, lines 23-26, 45-55).

As per claim 23, **Holloway** discloses a registration interface device (4a-c, 50), characterized in that it comprises: **Holloway** discloses *means for providing (11, 12) personal cryptographic data in said interface device* (see column 9, lines 18-26); **Holloway** discloses a client device connected to a system server 130 comprises at least two servers (see fig.1) through a network and discloses receiving a pass phrase (code) entered by a user the user at the client device (see column 8, lines 15-23 and column 9, lines 10-18) that meets the recitation of*, a means (6) for receiving (14) an authentic code entered by said user in said interface device*, **Holloway** discloses *a means for encrypting (20) said personal cryptographic data using said authentic code* (see column 9, lines 18-26);sending from a system server in which is stored users cryptographic data encrypted with users' pass phrase (see column 7, lines 30-53) that meets the recitation of *a means for sending (24) said encrypted personal cryptographic data from said* *interface device to a first server device (3) to store said encrypted personal cryptographic data in said first server device, in which the respective personal cryptographic data of a plurality of users is stored, said personal cryptographic data of each user being encrypted using a respective authentic code of said user,* **Holloway** discloses *receiving (42) the encrypted personal cryptographic data of said user in said interface device,* (see column 9, lines 18-26); **Holloway** also discloses that the pass phrase may also used as a key and stored in client as key or hashed (see column 8, lines 18-23, and lines 45-50) and erasing the algorithms and keys from the client (see column 7, lines 57-61 and column 10, lines 64-65) that meets the recitation of *a means for erasing (28) said personal cryptographic data and said authentic code from said interface device.*

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent 6,424,718 to **Holloway** in view of European Patent Publication 0535863 A2 to **Bellovin et al** *(Applicant's Disclosure)***.**

As per claim 7, **Holloway** discloses the client and server sharing a symmetric key and transmitting elements from the client to server and from the server to the client using verification data derived from authentication code entered by user (see column 8, lines 1-10) that meets the recitation of said first element of the group being transmitted to said first server device in an encrypted form using a distinguishing trace (VP) which derives from said code entered by the user in the interface device according to said deterministic function, said first element of the group being decrypted by said first server device using said personal code verification data (VP), said second element of the group being transmitted to said interface device in a form symmetrically encrypted using said personal code verification data, said second element of the group being decrypted by said interface device using said distinguishing trace. (see column 7, lines 30-47 and column 9, lines 47-55).

Holloway does not explicitly disclose using Diffie Hellman algorithm for the key distribution. **Bellovin et al** in an analogous art discloses exchange of keys using Diffie Hellman algorithm comprising chooses a first integer (a) corresponding to a first element (g.sup.a mod p) of a predefined group and said first server device chooses a second integer (b) corresponding to a second element (g.sup.b mod p) of said group, then said interface device and said first server device send each other said first and second elements, said interface device and said first server device each producing said at least one encryption key (Ks) (see pages 9-10). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Holloway** to send a random number from each party to generate the symmetric key because it would assure privacy and authentication as suggested by **Bellovin et al** (see section 3.3).

As per claim 8, the references as combined above disclose characterized in that said first and second elements of the group are encrypted with a symmetric encryption protocol (E) which is chosen such that an attempt to decrypt one of said elements of the group according to said protocol always produces an element of said group, whatever the data used in said attempt (see **Bellovin et al**, pages 9-10).

As per claim 9, the references as combined above disclose characterized in that said first and second elements of the group are encrypted with a symmetric encryption protocol (E) which is chosen such that said integer cannot be obtained from the corresponding encrypted group element (see **Bellovin et al**, section 3.2).

As per claim 10, the references as combined above disclose encrypting the elements using a symmetric encryption protocol and adding message authentication code and one-way function as verification data to prevent cryptanalytic attacks that meets the recitation of characterized in that said first element of the group, respectively said second element of the group, is encrypted with a symmetric encryption protocol (E) which comprises the step consisting in composing said element by a composition law of said group with the image of said distinguishing trace, respectively the image of said personal code verification data, by a function with values in said group (see **Bellovin et al**, sections 3.2-3.3 and 4.1).

8. **Claims 14-15** and **19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent 6,424,718 to **Holloway** in view of US Patent 6,970,562 to **Sandhu et al.**

As per claim 14, **Holloway** does not explicitly disclose imposing a delay. However, discloses a wireless client generating hash of a message (see column 84, lines 54-61 and column 85, lines 18-51) and a server at the other end verifying the message validity (see column 86, lines 16-43) using a first key that meets the recitation of generating a human-perceptible hash at the granting node and the requesting node, utilizing the first key; comparing the human-perceptible hashes via an out-of-band communication channel; **Sandhu et al** in an analogous art discloses imposing a system delay to defend against dictionary attacks (see column 17, line 55 through column 18, line 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Holloway** imposing a system delay so as to defend against dictionary attacks as suggested by **Sandhu et al** (see column 17, line 55 through column 18, line 3).

As per claim 15, the references as combined above disclose systematically monitoring (8) communications involving first server device (3) (see **Sandhu et al** column 17, line 55 through column 18, line 16).

As per claim 19, the references as combined above disclose rejecting (14) said authentic code entered by the user when said code satisfies predefined evidence criteria (see **Sandhu et al** column 18, lines 12-16).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-form 892).

9.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2136
August 20, 2008